Title:	Data Assurance Policy

Section 1: Introduction

1.1 Good quality information supports good quality decision-making. So good quality information is essential to Fylde Council. This policy sets out (in section 3) how the council ensures the quality of the information that it uses.

1.2 The council does not have a free hand in deciding what it does with the information that it keeps and uses. Under the Freedom of Information Act 2000, there is a presumption that all of the information held by the council should be available to the public on request. The council can only refuse a request for information in certain circumstances set out in the act. Conversely, under the Data Protection Act 1998, the council can only process personal data in accordance with that act.

1.3 This policy therefore also describes (in section 4) how the council complies with its obligations under the Data Protection Act to properly protect the information that it holds and (in section 5) the steps it has taken to make it easier to know how particular items of information should be dealt with.

1.4 This policy applies to all staff. As a matter of good practice, agencies and individuals working with the Council, and who either provide information to the council or have access to personal information held by the council, will be expected to have read this policy and comply with those parts that apply to them. Directorates who deal with such external partners should ensure that they agree to do so.

Section 2: Definitions

Personal Data

Any information relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. This includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Personal Data

Personal data that relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive personal data is subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data,

including decisions regarding the purposes for which personal data is processed and the way in which it is processed. The Council is the data controller for the purposes of this policy

Data Subject

A person who is the subject of personal data.

Processing

Virtually anything that can be done to data, including accessing, altering and destroying it.

Third Party

Any individual/organisation other than the data subject, the data controller (the Council) or its agents.

Section 3: Data Quality

3.1 Every employee has a responsibility for information quality whenever they record, use or publish information. Directors have an overall responsibility for making sure that their directorate has appropriate practices and procedures for ensuring the quality of information recorded, used or published by their directorate. Recording information includes making a record of it on paper, electronically or by any other media. Using information includes making decisions based on it, or presenting it (for example, as part of a report) to somebody else. Publishing it means making it available to the public or a section of the public.

3.2 Good quality information is **accurate**, **available** and **useful**.

Accurate:

3.3 If the information is factual, it should be true insofar as the person recording it and the person using it can reasonably ascertain. If the information is opinion, it should represent the true and reasonable view of the person providing it and should be identifiable as opinion in the context it is used.

3.4 There should be enough information for the purpose, but not too much. Incomplete information can sometimes be misleading. But presenting too much information can lead to confusion.

Available:

3.5 If information is not available, it might as well not be kept. Information is only available if it is both physically accessible and searchable.

3.6 Information is searchable if there is some system for finding it and (where appropriate) finding out what is in it. This need not be electronic, and could include manual catalogues or indexes. But it should not be left to the memory of individuals, as individuals can forget or leave the council.

3.7 Information is only available if someone has not taken it away. So there should be appropriate processes to ensure the security of information. These will vary depending on the information involved. However, there are specific legal requirements about

security of personal data. These are dealt with in more detail under section 4 (data protection).

Useful:

3.8 Information is only useful if it is up-to-date for the purposes for which it is to be used and can be understood.

3.9 Modern technology makes it easier to access up-to date information and less necessary to keep a local copy of it. For example, it will almost never be necessary to keep a paper copy of a document that is available online. Information should always be checked for accuracy before it is published or used.

3.10 Information that cannot be understood by its audience is not useful. Highly technical information should be summarised or accompanied by an explanation if it is intended for a lay audience.

Section 4: Data Protection

4.1 The Council is committed to protecting the rights and privacy of individuals (including customers, staff and others) in accordance with the Data Protection Act. The Council needs to process certain information about its staff, customers and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to carry out its functions, and to comply with legal obligations). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

4.2 This part of the policy sets out what you need to do to help the council comply with its legal obligations. It does not repeat the whole of the law about data protection. You can get advice that is more detailed from the Head of Governance, who is the Council's lead officer for data protection.

4.3 The Council has to register with the Information Commissioner as a body that holds personal data. The Head of Governance keeps the Council's registration up to date. Details of the Council's registration are published on the Information Commissioner's website. The entry lists all of the purposes for which the council processes data. If you intend to process data for purposes not included in the Council's registration, you should seek advice from the Head of Governance.

Data Protection Principles

4.4 You must only process personal data in accordance with the eight data protection principles. These are contained in the Data Protection Act and summarised here:

1. ***Personal data shall be processed fairly and lawfully.***
   Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period

for which the data will be kept.

2. ***Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.***
   Data obtained for specified purposes must not be used for a purpose that differs from those.

3. ***Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.***
   Information which is not strictly necessary for the purpose for which it is obtained should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

4. ***Personal data shall be accurate and, where necessary, kept up to date.***
   Data which is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate.

5. ***Personal data shall be kept only for as long as necessary.*** *(see the section on Retention and Disposal of Data)*

6. ***Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.*** *(see the section on Data Subjects' Rights)*

7. ***Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.***
   (see the section on Security of Data)

8. ***Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.***
   You should be particularly aware of this when publishing information on the Internet and when using data processing services or cloud-based storage, whose servers may be outside the EEA.
   The European Economic Area (EEA) is the EU Member States together with Iceland, Liechtenstein and Norway.
   The European Commission has formally decided that the EU-US Privacy Shield provides an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This means the council can transfer data to an organisation in the United States if the organisation receiving the data is certified under the EU-US Privacy Shield.

Data Subject Rights

4.5 Data Subjects have the following rights concerning personal data about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.

- To be informed about mechanics of automated decision taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

Processing Personal Data

4.6 The Council can generally only collect use or disclose data if one of the conditions summarised in this section applies:

- It is necessary in connection with a contract with the data subject
- It is necessary so that the Council can comply with a legal obligation (except a contract)
- It is necessary to protect the vital interests of the data subject: that is, a medical emergency
- It is necessary for the administration of justice
- It is necessary to perform a statutory function
- It is necessary to perform a public function on the public interest
- It is necessary for the legitimate interests of the council or a third party to whom the data is disclosed – but this must be balanced against the legitimate interests of the data subject
- The data subject has given their active consent

4.7 If you are in any doubt about whether data can be processed in a particular way, get advice from your manager or the Head of Governance

Security of Data

4.8 You must make sure that any personal data which you deal with is kept securely and is not disclosed to any unauthorised third party (see the section on Disclosure of Data for more detail).

4.9 All personal data should be accessible only to those who need to use it. You should form a judgement based upon the nature of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet, or
- if computerised, password protected, or
- on removable media which are themselves kept securely.

4.10 Take care that PCs and laptops are not visible except to authorised staff and that computer passwords are kept confidential. Do not leave PC screens unattended without

password protected screen-savers. Don't leave manual records where they can be seen by unauthorised personnel.

4.11 Put appropriate security measures are in place for deleting or disposing of personal data. Shred manual records or dispose of them as "confidential waste". Wipe clean or destroy hard drives of redundant PCs before disposal.

4.12 This policy also applies to processing of personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Take particular care when processing personal data at home or in other locations outside the Council's offices. Personal data should never be taken off site on a device or storage medium that is not encrypted.

4.13 Do not store personal data belonging to the council in a cloud-based storage facility without the specific consent of your Head of Service, who should consult with the council's IT section.

Rights of Access to Data

4.14 Data subjects can request access any personal data about which the Council holds about them. If you receive a request, you should ask for it to be put in writing and either:

- refer the request to the Head of Governance, or
- if the request is specific to information that you control, disclose it (but only after making sure that the person requesting it is the data subject)

4.15 The Council reserves the right to charge a fee for data subject access requests (currently £10). Any such request must be complied with within 40 days of receipt of the written request and, where appropriate, the fee. There are some exemptions to the right to access personal data. If you feel that an exemption may apply, contact the Head of Governance.

4.16 The right to request access applies to any personal data held about a person. However, if the data is not kept or ordered by reference to individuals, the data subject would normally have to say what data they wish to see. The Council could refuse the request if complying with it exceeds a cost limit set by government.

Disclosure of Data

4.17 The Council must ensure that personal data is not disclosed to unauthorised third parties, which include family members, friends, government bodies, and in certain circumstances, the Police. You should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. Nor would it be appropriate to give home contact information. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of Council business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of staff concerned.

4.18 As well as the conditions listed in 4.6, there are some other specific instances where disclosure to a third party is allowed. These concern national security, crime and taxation and regulatory activity. If any issue arises about these, or if in doubt, ask for advice from your executive manager or the Head of Governance.

4.19 There are some other exemptions not listed here which would be unlikely ever to arise.

Retention and Disposal of Data

4.20 The council has a separate policy on data retention, based upon guidance and classifications provided by the Information and Records Management Society.

Section 5: Data classification

5.1 The council has adopted a simple classification system to make it easier to identify how information that it holds should be treated. The system is intended to reflect the statutory position under the Data Protection Act 1998 and the Freedom of Information Act 1990. The council considers that any advantages of introducing a more complex system of classification would be outweighed by the burden of implementing such a system.

5.2 The classifications are:

- **Personal Information**: This is information that is personal data or sensitive personal data as defined under the Data Protection Act 1998. In other words, it is information that the council cannot (except with the consent of the data subject or in certain other limited circumstances) disclose
- **Excluded Information**: This is information that, on an application for disclosure under the Freedom of Information Act 2000, would be likely to be withheld from disclosure under any of the exemptions other than the exemption applicable to personal data. In other words, it is information that the council may, but need not, disclose.
- **Unrestricted Information**: This is information that, on an application under the Freedom of Information Act 2000, the council would be obliged to disclose.

5.3 From the implementation of this policy, employees will be encouraged to discreetly mark Personal and Excluded Information so that users of that information will be alerted to its status. Unrestricted Information may also be marked as such. Marking an item of information as Personal, Excluded or Unrestricted will not be conclusive of its status. An employee using any information must always consider the principles set out in this policy, as well as the requirements of the Data Protection Act 1998.

5.4 Where an item is marked as Excluded Information, it must not normally be published or disclosed without first giving full consideration to how the council's interests (or the interests of any other person who might be affected by the publication or disclosure) might be affected if it was published or disclosed.

5.5 Where an item is marked as Personal Information, it must not be published or disclosed (except to the data subject) without the approval of the relevant head of service.

Section 6: Monitoring and Review

6.1 The council's Management Team will monitor and keep this policy under review. They will judge its success by the following criteria:

- The quality of information available to decision-makers
- Compliance with the council's obligations as data controller under the Data Protection Act 1998
- The balance between the advantages secured by the policy and the burdens imposed by it.